Yoti MyFace ® Liveness

White Paper | Full version

May 2025

Introduction

The growing use of biometric and authentication solutions, online and offline, has raised the risk of 'spoofing' attacks, an attempt to spoof the system with an artificial representation. Having robust technology to mitigate against spoofing is essential as part of a mix of tools to verify someone. This is true whether that be for verifying age, identity or authenticating a returning customer.

The purpose of liveness is to make sure the person you are verifying is present in front of the device camera in real time. This is also sometimes known as Presentation Attack Detection (PAD). Liveness does not recognise who the person is (that is facial recognition). It is most commonly used in combination with other authentication factors to ensure that authentication or verification isn't being spoofed.

> **"The purpose of liveness is to make sure the person you are verifying is a real person"**

In combination with wider AI services, liveness can help provide stronger security for individuals and businesses for verification and authentication. Attempts to spoof a verification process are significantly more difficult to achieve when liveness is incorporated as part of the process.

Liveness combats what is technically termed "presentation attacks". Without liveness, you are susceptible to a presentation attack. Such attacks include:

- Paper image
- Mask
- Screen image
- Video imagery
- Deepfake video
- Injection attacks
- Bot attacks
- Injection attacks

We have found that genuine customers do not object to efficient and effective security layers. In fact most customers appreciate companies taking the time and effort to ensure their assets, accounts, or finances are being looked after and kept safe.

Where can it be used?

Identity Verification - used as part of the verification process to give a high confidence that the check is real.
Why important? - a stolen document plus an image could spoof an identity check.
Example use case - your customer wants to sign up to a new bank account and is required to prove their identity. Liveness ensures the person signing up is a real person. Liveness is used in combination with data extraction, document authenticity and face match for a secure verification process.

Age Verification - ensuring the person is not only the right age but also not attempting to spoof the system with a presentation attack. This could be used online or offline (for example, at a supermarket self-checkout).
Why important? - to strengthen age verification and provide quick, privacy-preserving age checks.
Example use case - a shopper uses facial age estimation at a supermarket self-checkout. Liveness prevents someone from attempting to use a picture, mask or other spoofing attack to pass an age check. For online applications, it ensures industries, such as gaming and social media, know the person proving their age is a real person.

Digital ID - to create a reusable Digital ID we require a high level of confidence to determine: the document data extraction, document authentication, the document belongs to that person and finally that the person is real.
Why important? - pre-verified, reusable Digital ID provides the highest level of security and confidence that a business knows who they say they are.
Example use case - A returning customer can easily access their account, and the business can be confident the customer is who they say they are.

Authentication - liveness can be an additional form of authentication for high risk / regulated environments, adding an extra layer which makes it harder for spoofers to scam.
Why important? - multi-factor authentication is now required by many regulators and an efficient, low friction way to do this is actually desirable for customers.
Example use case - a genuine customer is accessing their account, or changing important information such as their bank details. A liveness check can add an authentication layer with low friction - key for sensitive account changes and to help prevent account takeovers.

Bot Detection - checking for liveness when capturing a face helps prevent bad actors from submitting hundreds or thousands of synthetic faces, or genuine, but unconsented faces.
Why important? - the financial and reputational cost to businesses from bot attacks can be significant.
Example use case: dating app Muzz uses liveness to confirm every account profile belongs to a real person. Liveness has eliminated bots and increased user trust when engaging with other young people in the Yubo community.

Types of liveness - active and passive

Active liveness requires the user to present their face on camera and then follow one or more instructions during a check; for example, moving their head toward and away from the camera, looking to the left and right, smiling, or repeating random words. Then AI is used to complete the check.

This can create issues for some users, for example the words may not be in their native language, and adding movement to the check increases the margin for error. Additionally, not all individuals follow instructions carefully and the rapid development of deepfake AI enables bad actors to mimic the given instructions in real time.

In general, the simpler the instruction and the less user time required, the better the user experience and completion rate. Passive liveness takes between on average 1 second, with active liveness taking between 15-20 seconds.

Passive liveness doesn't require any action from the user and works from a single selfie. Users no longer have to undertake head or hand movements to prove their 'liveness'. This reduces friction for users. It is simpler for people with accessibility needs and so more societally inclusive. This reduces drop off and speeds up the journey to verifying genuine customers.

A comparison between passive and active liveness

	Passive	**Active**
User feedback	Instant feedback	User has to wait for video validation
Time to complete	1 second average	15-20 seconds
Complexity and accessibility	Take a selfie - this can be either using auto face capture or at the click of a button.	User has to record a video and maintain the correct position for the duration. Language, audio input and noisy environments can be a problem for some users.
Permissions	Camera access	Camera & audio record
Network traffic	Upload a selfie	Upload a selfie & video

Yoti MyFace® proprietary liveness

Yoti MyFace® is a passive liveness software that uses a selfie image to detect presentation attacks. It doesn't require any action from the user and just works from a selfie, which is processed through a sequence of deep neural networks.

The network has been trained using a variety of models that analyse images in a different way. We have invested considerable time and effort over years to fine tune these models to optimise how they work together to create world class performance.

As an example, one of these models, for which we have filed a patent in August 2018, uses 3D and 2D images as input to produce a model that can detect depth in a 2D image.

How passive liveness works

From a user perspective, they are just taking a selfie. Behind the scenes there is a considerable amount of technology working to ensure a successful outcome for both users and organisations. This is all processed on average in under one second.

1. **Image capture**: in real-time, AI models ensure the best image is captured for processing, by analysing the position of the face - where head on, and not tilted or angled, is optimum.

2. **Image fidelity**: simultaneously, in real time, the image capture assesses the quality of the image, in terms of lighting or blurriness - giving real time feedback if required.

3. **Secure Image Capture (SICAP)**: to ensure the image is genuine, SICAP detects whether the image itself is being captured, live, from the device camera, or has been subjected to an injection attack. See page 9 for further details.

4. **Liveness assessment**: the resulting image is cropped many times to produce the inputs for the relevant neural network models and is then processed using multiple models (over 10 simultaneously).

5. **Data processing**: results from each model are assessed together to produce a response and a confidence level that the image is of a real person.

6. **Results**: a response is returned **on average in 1 second**. Relying parties are able to configure their checks to pass only above a given confidence level, depending on their risk profile and regulatory requirements of the territories in which they operate.

MyFace® performance - true positive and true negative rates

We measure performance in terms of true-positives, and false-positives, success rates and completion times.

- When our model predicts that a real image is real, that is a true-positive (TPR).
- When our model predicts that an attack image is real, that is a false-positive (FPR).
- The aim is for a high true-positive rate, and a low false-positive rate.

Taking in combination the ease of access, time to complete, immediate feedback and ease of use, passive liveness significantly improves success without compromising security.

On mobile phones, 92% of first attempts are successful, 97% after 3 attempts.

MyFace® performance in live environments

We have been using MyFace® in our facial age estimation solution, alongside other liveness providers. We complete millions of liveness checks every day in real world settings which in turn, enables us to gather vast amounts of information on emerging threats.

We perform liveness across a variety of environments and applications. Performance is influenced by camera quality, image size, and environmental factors.

For example, during the Home Office trial in supermarkets in the UK, we were able to gain further intelligence on how the use of our technology on self-checkouts can be adversely affected by factors such as sun glare, overhead lighting and camera positioning in the self checkout.

This also explains the discrepancy between the mobile only first attempt rates of 92%. Compared to laptop cameras and self-checkouts, mobile phones tend to have a high quality camera and many users are used to taking ‘selfies’ on their phone.

92%

Pass rate on 1st attempt

97%

Total pass rate

Success rates - improvements over time

Our experience with providing verification solutions demands a capability of continual improvement due to a developing fraud environment.

As you can see below, over the last two years our success rates for passive liveness have improved significantly from a blended (mobile and desktop) view of 89% to 92% on the first attempt and 93% to 97% by the third attempt.

What is also notable is the shift, from our experience, to the use of mobile devices, as represented in the blended percentage, where the influence of desktop has lowered over time. This reflects how consumers and operators are deploying our products and how device usage is developing, for both active and passive liveness methods. It also reflects the quality and efficacy of mobile device cameras, as well as the ease of use and familiarity of 'taking a selfie', on mobile devices.

Passive and active liveness success rates improvements over time

		Passive liveness		Active liveness	
		Mar 23	May 25	Mar 23	May 25
After one attempt	Mobile	89%	92%	74%	76%
	Desktop	78%	90%	56%	60%
	Blended	89%	92%	72%	75%
After three attempts	Mobile	95%	97%	83%	87%
	Desktop	87%	94%	67%	68%
	Blended	93%	97%	81%	85%

Third party testing: NIST levels 1 and 2

NIST is the National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce. NIST provides a framework for testing performance levels of liveness.

NIST Level 1 involves testing against materials that could be found in a normal home or office. Materials used for testing should not cost more than $30. Masks are excluded.

To pass NIST Level 1, the Liveness service must detect every attack and limit false negatives to less than 15%. We were tested with over 900 attacks and our tested MyFace® model was not allowed to have one false positive.

In February 2022, MyFace® achieved NIST level 1 certification with 100% attack detection rate. We worked with iBeta, a NIST NVLAP accredited biometrics testing lab, for our level 1 compliance.

NIST Level 2 involves testing against more expensive, specialist attacks, such as 3D printers, and resin or latex face masks. Materials used for testing should not cost more than $300.

To pass NIST Level 2, the service must detect 99% of attacks and limit false negatives to less than 15%. False negatives occur when a system rejects a genuine user incorrectly.

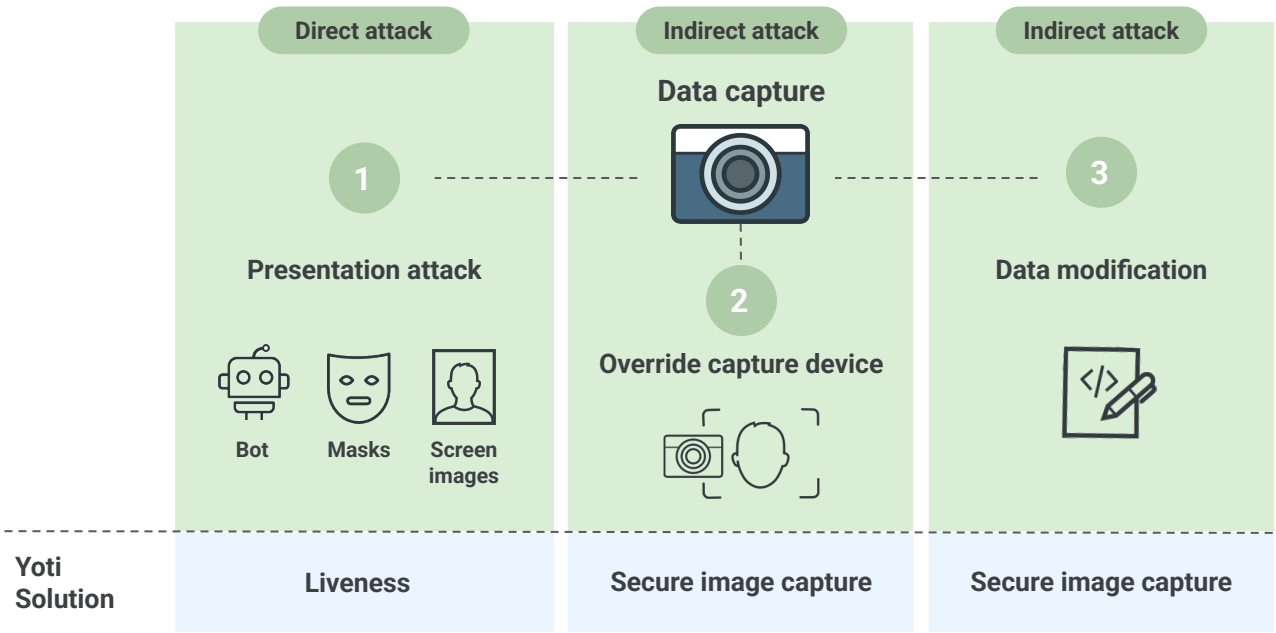
In February 2023, MyFace® achieved NIST Level 2 compliance, again working with iBeta, with 100% attack detection rate.

The threat of injection attacks

An important question for any new technology, is how secure is the process? Can it be spoofed, are bad actors able to hack into the system to override checks, images or results?

This is why it is important to use a combination of technologies to secure a high level of assurance. There are a number of threat vectors, as illustrated in the diagram below.

Data capture attack threats



Step 1 as a direct spoofing attack - an attempt to present an image, mask or video, often called a presentation attack. This is an attempt to spoof a check by appearing older or to be another person. To overcome this we use our NIST 2 certified liveness technology[9]. This ensures that the person undertaking the check is a real person and not someone wearing a mask, or presenting to the camera a picture or screen of another (older or younger) person.

Steps 2 & 3 is a newer, more sophisticated, but relatively easy way for technically competent individuals to spoof the system. They are called injection attacks. An injection attack involves injecting an image or video designed to pass authentication, rather than the one captured on the device camera. Using free software and some limited technical ability, a bad actor is able to overwrite the image or video of the camera with pre-prepared images.

In 2020, Yoti recognised the upcoming risk of injection attacks and started to develop a solution, called SICAP (**S**ecure **I**mage **CAP**ture). Our patent for SICAP was granted in Noember 2023, which makes injection attacks significantly more difficult for imposters[10].

Our experience of rising fraud trends and injection attacks

In 2024, we witnessed a significant increase in the number of deepfake attacks, or injection attacks during age and identity verification checks. The percentage of attacks increased from 1.6% to 3.9%.

In absolute terms, this is a significant rise in the total number of attacks we have detected as we significantly expanded our services in 2024. We now perform over 7 million checks per week across all our services. With the introduction of various regulations globally, companies have been obliged to implement more robust age or identity checks for their users.

We have seen injection attacks across identity verification and facial age estimation across the Yoti network rise from a daily average around 1,000 attacks in February 2024 to a daily average of over 6,000 attacks in January 2025.

Yoti memberships, associations, accreditations & awards

To learn more about Yoti MyFace® liveness and our AI Solutions please **get in touch**.